Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Managed Service Providers: How to Manage Risk to Customer Networks

First published: December 2018
Last updated: October 2021

Introduction

The compromise of several Managed Service Providers (MSPs) was reported in 2017. In response, the Australian Cyber Security Centre (ACSC) provided organisations with the information they needed to protect themselves and others from this threat.

In 2018, adversaries continued to target and compromise MSPs and, through them, their customers. The ACSC reiterates the need for organisations to scrutinise the cyber security measures implemented in contracted ICT solutions to combat the threat.

Mitigation strategies

Many of the compromises involving customers of MSPs occurred because MSPs themselves were the initial point of compromise. That is, the customer was not the initial victim; the MSP was the vector to compromise their customers. An MSP must manage the security risks they pose to their customers' systems by protecting their own network from basic intrusion attempts, and by protecting the trust relationship with a customer.

This publication provides strategies MSPs can implement to protect their own networks and manage the security risks posed to customer networks. Note that many of these recommendations apply to any outsourced ICT service provider, not just MSPs. The number and type of controls an MSP will utilise with their customers will vary depending on the sensitivity of the customer's systems and data.

Ensure your own network is secure

Determine if you have been affected by the recent campaign targeting MSPs. Resources are available from the US's Cybersecurity & Infrastructure Security Agency and the UK's National Cyber Security Centre. MSPs should fully investigate any indications of a cyber security incident and report any malicious activity to the ACSC.

Be aware that an absence of specific indicators of compromise (IOC) is not evidence of the absence of a cyber security incident. Adversaries can utilise different tools and infrastructure in different victims, particularly when IOCs are publicly or broadly exposed.

Implement a cyber security standard within your own organisation, and promote it in the systems you manage for your customers. For example, the Essential Eight is a prioritised list from the ACSC's *Strategies to Mitigate Cyber Security Incidents*. These strategies are effective in defending against malicious activity such as preventing the execution of malware and reducing the attack surface of an organisation.

Have an upfront and transparent cyber security conversation with your customers

MSPs have a responsibility to protect their customers' data, which includes notifying them of cyber security incidents. MSPs should be transparent when a cyber security incident occurs, including what steps they should take to remediate and mitigate the risk of the cyber security incident reoccurring.

Ensure mutually agreed cyber security expectations. MSPs should ensure a discussion about what security a customer can expect is part of the negotiation and ongoing relationship. This should be a differentiator for a good MSP.

Include cyber security incident notification clauses in your contract with your customer. The MSP must notify the customer in the event of any cyber security incident that may endanger the customer network. This may include cases in which MSP systems related to the administration, management or storage of information on the customer network have been compromised or accessed by an unauthorised and/or unknown party. MSPs must consider reporting obligations required by mandatory breach disclosure legislation in Australia.

Understand the security clearance level expected of MSP staff working on customer systems. There is additional risk to customers from insider threats if staff are engaged outside a customer's security clearance and background checking procedures.

Securely administer access to customer systems

To perform their contracted duties, an MSP may administer either a system on a customer network or their entire network. Without proper controls, this high level of privileged access, combined with potential dependency of a customer on the security of the MSP network, can leave customer networks and data vulnerable to intrusion.

Know where the boundaries are between you and your customers. Ensure that you clearly identify which customer systems you administer and how, and keep the record up to date.

Segment the customer network from the MSP's. This will limit an adversary's ability to move laterally from a compromised MSP network into any customer network and vice-versa. The ACSC has observed adversaries using compromised MSP workstations to move laterally to customer networks, including critical systems such as Windows Domain Controllers. Examples of segmentation include:

- Where an MSP administers an entire network, the MSP network should not be used to administer a customer's systems. Instead, MSP staff should administer the customer's network from a system within the customer's network.
- Consider segmenting your network into trust zones.

Segment customers from each other, or into risk domains. Ensure that a customer with a high security requirement is not co-hosted or co-managed with low security or higher risk customers. At a minimum, ensure that a customer is aware that they are hosted in a low security assurance area. An example of this behaviour is shared web hosting. In 2018, the ACSC investigated multiple web hosting providers that were compromised through a vulnerable web service on one client that then compromised the underlying infrastructure due to its poor security configuration, which led to the compromise of all websites hosted on that service.

Utilise a secure jump host to perform administrative tasks. If you must access a customer network from your own network, or remotely, specify a dedicated workstation on which your administrative staff should perform sensitive administration duties, with restricted access to critical servers. Combine this with multi-factor authentication to limit an adversary's ability to compromise critical assets.

Mitigate the impact of stolen or abused credentials

The theft and abuse of credentials is presently a common and effective intrusion vector. Credential theft does not necessarily require the internal network to be compromised, for example, phishing pages and NTLM credential leaks are alternative methods. Typically, when an adversary has full access to an MSP they will have access to all the credentials on their network. This not only includes corporate credentials of the MSP, but likely also credentials for their client's devices and systems managed by the MSP, if they are stored or accessed on the MSP systems.

Credential management is part of controlling and restricting MSP access to customer networks, and limiting the consequence of stolen credentials.

Implement least-privilege administration on customer systems to decrease the impact of adversaries gaining MSP-level access to customer networks. Use the least privileged account(s) required to administer customer networks.

Strongly control enterprise and domain administrator accounts. Enterprise and domain administrator accounts should have no members by default. Utilise just-in-time principles for privileged accounts like the domain administrator. Use a manual process or privileged access management software to add named accounts to the domain administration role, for a limited duration.

Provide attributable accounts. Accounts should be attributable to the MSP to enable easy identification of MSP activity in privilege allocation and logs. The ACSC has observed adversaries using legitimate support accounts provisioned by MSPs to deploy malware to customer networks; rapid attribution of such activity would assist the customer to work with their MSP to remediate compromises of their network.

Enable multi-factor authentication on remotely accessible services used to access customer networks and systems. This will ensure that, even if an adversary has compromised credentials of MSP accounts, they remain incapable of logging on without a second factor such as a hardware token. Adversaries have used Remote Desktop Protocol directly from a MSP network to deploy malware to servers anywhere in an administered network.

Record and review MSP actions on customer networks

Why collect log data

Good logging is essential for conducting an effective investigation, reducing the overall cost of responding to cyber security incidents.

Data collection considerations

Log data should be collected from diverse sources in order to enable correlation and validation of events. Some data sources and events within those sources are more valuable than others, so consideration should be made to prioritise data collected if storage space is a concern.

Log data should be centralised into one system for correlation, have the ability to be queried with standard alerting and customised queries, and be reviewed.

The following types of data are useful to an investigation:

- host-based event logs to provide visibility of malicious activity on workstations and servers
- firewall and proxy logs to provide visibility of network connections associated with adversaries
- remote access logs to identify abuse of legitimate external access.

Maintaining default sizes of event logs, when stored on a local system, may cause older logs that contained key data to be overwritten prior to commencing an investigation; it is therefore advised that organisations increase the default sizes or forward logs to a central location for storage.

Based on ACSC experience in cyber security investigations, a minimum of 18 months logging assists investigations.

MSP and their customers' data

In addition to monitoring an MSP's own network, an MSP must monitor their access to their customer networks.

Consider scheduling remote access to customer networks at an agreed time and correlating logs with a specific job ticket.

Be prepared to provide detailed logs related to customer systems if a customer has security concerns they wish to investigate further.

Plan for a cyber security incident

Have a practical incident response plan

If you detect a cyber security incident, or have been notified of a possible cyber security incident, ensure you get as much detail as possible. Look for indications of what security vulnerability enabled the cyber security incident to occur. For example, a web-facing scan of services is very different to an unauthorised external system logon, or internal lateral movement. Relevant information will ensure accurate prioritisation and messaging. This information may include:

- What sort of cyber security incident is it?
- What specific data and systems are known to be affected?
- What was the indication that there was a cyber security incident?
- What was the date and time of the cyber security incident?
- Is the cyber security incident ongoing?
- What actions are being taken to investigate and remediate?
- Has this cyber security incident been reported anywhere?

Have a communications strategy

If a cyber security incident occurs, and it likely affects customer data, it is better to be open and transparent with customers and steer the response than to wait. If customer data has been stolen, there is a high probability that a third party will discover the cyber security incident because the adversary is often less interested in your security and the security of your customers' data.

Communicate securely. If the compromise involved your corporate network, you may no longer be able to trust corporate communications. Particularly early in an investigation, ensure you have alternate secure communication channels internally and with your customer. Keep records of any engagement with the customer for future reference.

Report to the relevant authorities. Ensure that the appropriate person(s) within your organisation have been notified. If personal information has been lost or compromised, you may be legally required to report the cyber security incident to the Office of the Australian Information Commissioner. You should also report the cyber security incident to the ACSC for advice and assistance on how to remediate your network, as well as to both contribute to and benefit from the ACSC's broad situational awareness.

If the cyber security incident is reported publicly, or is made public during or after an investigation, have public talking points pre-prepared. If other stakeholders are mentioned in the public communication, ensure they are consulted or notified as soon as possible.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Further information for customers on questions they can ask MSPs prior to engaging their services is available in the *Questions to Ask Managed Service Providers* publication.

Further information on outsourcing services to cloud service providers is available from the ACSC.

The US Cybersecurity & Infrastructure Security Agency has also produced guidance on mitigating the risks of engaging with MSPs.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).